PATENT COOPERATION TREATY

PCT

INTERNATIONAL PRELIMINARY REPORT ON PATENTABILITY

(Chapter II of the Patent Cooperation Treaty)

(PCT Article 36 and Rule 70)

Applicant's or agent's file reference JIM/PL/2040553/at	**FOR FURTHER ACTION**	See Form PCT/IPEA/416
International application No. **PCT/SG2005/000084**	International filing date *(day/month/year)* 17 March 2005	Priority date *(day/month/year)* 17 March 2004

International Patent Classification (IPC) or national classification and IPC

Int. Cl.

G06F 12/14 (2006.01) ***G06K 19/073*** (2006.01) ***H04L 9/18*** (2006.01)

Applicant

DIGISAFE PTE LTD et al

1. This report is the international preliminary examination report, established by this International Preliminary Examining Authority under Article 35 and transmitted to the applicant according to Article 36.
2. This REPORT consists of a total of 4 sheets, including this cover sheet.
3. This report is also accompanied by ANNEXES, comprising:

   a. ☒ *(sent to the applicant and to the International Bureau)* a total of **5** sheets, as follows:

   ☒ sheets of the description, claims and/or drawings which have been amended and are the basis for this report and/or sheets containing rectifications authorized by this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions).

   □ sheets which supersede earlier sheets, but which this Authority considers contain an amendment that goes beyond the disclosure in the international application as filed, as indicated in item 4 of Box No. I and the Supplemental Box.

   b. □ *(sent to the International Bureau only)* a total of (indicate type and number of electronic carrier(s)) , containing a sequence listing and/or table related thereto, in electronic form only, as indicated in the Supplemental Box Relating to Sequence Listing (see Section 802 of the Administrative Instructions).

4. This report contains indications relating to the following items:

☒	Box No. I	Basis of the report
□	Box No. II	Priority
□	Box No. III	Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
□	Box No. IV	Lack of unity of invention
☒	Box No. V	Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
☒	Box No. VI	Certain documents cited
□	Box No. VII	Certain defects in the international application
□	Box No. VIII	Certain observations on the international application

Date of submission of the demand 17 January 2006	Date of completion of this report 14 July 2006
Name and mailing address of the IPEA/AU AUSTRALIAN PATENT OFFICE PO BOX 200, WODEN ACT 2606, AUSTRALIA E-mail address: pct@ipaustralia.gov.au Facsimile No. (02) 6285 3929	Authorized Officer **R. W. J. FINZI** Telephone No. (02) 6283 2213

INTERNATIONAL PRELIMINARY REPORT ON PATENTABILITY

International application No.
PCT/SG2005/000084

Box No. I   Basis of the report

1. With regard to the **language,** this report is based on:

☒ The international application in the language in which it was filed

☐ A translation of the international application into , which is the language of a translation furnished for the purposes of:

☐ international search (under Rules 12.3(a) and 23.1 (b))

☐ publication of the international application (under Rule 12.4(a))

☐ international preliminary examination (Rules 55.2(a) and/or 55.3(a))

2. With regard to the **elements** of the international application, this report is based on *(replacement sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to this report)*:

☐ the international application as originally filed/furnished

☒ the description:

pages **1, 5 - 12** as originally filed/furnished
pages* **2 - 4** received by this Authority on **17 January 2006** with the letter of **17 January 2006**
pages* received by this Authority on with the letter of

☒ the claims:

pages as originally filed/furnished
pages* as amended (together with any statement) under Article 19
pages* **13 - 14** received by this Authority on **17 January 2006** with the letter of **17 January 2006**
pages* received by this Authority on with the letter of

☒ the drawings:

pages **1 - 2** as originally filed/furnished
pages* received by this Authority on with the letter of
pages* received by this Authority on with the letter of

☐ a sequence listing and/or any related table(s) - see Supplemental Box Relating to Sequence Listing.

3. ☐ The amendments have resulted in the cancellation of:

☐ the description, pages
☐ the claims, Nos.
☐ the drawings, sheets/figs
☐ the sequence listing *(specify)*:
☐ any table(s) related to the sequence listing *(specify)*:

4. ☐ This report has been established as if (some of) the amendments annexed to this report and listed below had not been made, since they have been considered to go beyond the disclosure as filed, as indicated in the Supplemental Box (Rule 70.2(c)).

☐ the description, pages
☐ the claims, Nos.
☐ the drawings, sheets/figs
☐ the sequence listing *(specify)*:
☐ any table(s) related to the sequence listing *(specify)*:

* *If item 4 applies, some or all of those sheets may be marked "superseded."*

Box No. V **Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement**

1. Statement

Novelty (N)	Claims **1 - 7**	**YES**
	Claims **Nil**	**NO**
Inventive step (IS)	Claims **1 - 7**	**YES**
	Claims **Nil**	**NO**
Industrial applicability (IA)	Claims **1 - 7**	**YES**
	Claims **Nil**	**NO**

2. Citations and explanations (Rule 70.7)

Novelty (N) and Inventive Step (IS):

D1) US 2002/0188856 A1 (Worby) 12 December 2002
D2) WO 2001/035193 A1 (INTERNATIONAL BUSINESS MACHINES CORPORATION) 17 May 2001
D3) US 6199163 B1 (Dumas et al.) 6 March 2001
D4) EP 911738 A2 (CALLUNA TECHNOLOGY LIMITED) 28 April 1999
D5) US 2003/0177379 A1 (Hori et al.) 18 September 2003
D6) WO 2003/012606 A2 (STONEWOOD ELECTRONICS LTD) 13 February 2003
D7) WO 2000/079392 A1 (FOTONATION, INC) 28 December 2000

None of the citations disclose the invention as claimed. The closest prior art, that of D4, describes a disk drive having an encryption/decryption circuit and security control means. Paragraph 27 discusses user authentication, and states that on power up, the drive is in the disabled state and is placed in the enabled state by inputting a numerical key that acts like a password. The numerical key is authenticated by the encryption hardware on the drive. If the numerical key is valid read/write access to the drive is granted, but if the numerical key is invalid then such access is denied. Consequently, there is no disclosure of the memory being exposed prior to user authentication.

Industrial Applicability (IA):

The claimed invention finds use in the field of data storage and clearly meets the requirements for industrial applicability.

Box No. VI Certain documents cited

1. Certain published documents (Rule 70.10)

Application No. Patent No.	Publication date *(day/month/year)*	Filing date *(day/month/year)*	Priority date (valid claim) *(day/month/year)*
D1) P,X US 2004/0103288	27 May 2004	27 November 2002	27 November 2002

Claim 6 is not considered to be novel or inventive in light of citation D1, which discloses a method of protecting data in which an encryptor is exposed to an interface only upon successful user authentication. In D1, it is noted that memory area 121 is exposed to the interface at least until user authentication (please refer to paragraph [0037] and Figure 6). If user authentication is successful, then memory area 122 is exposed for the storage of data.

2. Non-written disclosures (Rule 70.9)

Kind of non-written disclosure	Date of non-written disclosure *(day/month/year)*	Date of written disclosure referring to non-written disclosure *(day/month/year)*

associated with the software solutions described above, these hardware solutions cannot be easily implemented on portable computing devices such as notebook computers because additional interface hardware cannot be accommodated in the space normally occupied by, in a notebook computer, a hard disk. In addition, these hardware solutions often require an additional interface into which a hardware key is inserted in order to authenticate the user to the hardware encryptor before activating the hardware encryption/decryption device. This interface is necessary because the hardware solution has no way of interfacing to other authentication devices, such as keyboards. This hardware interface cannot, therefore, be implemented on the portable computing device without customizing the device.

SUMMARY OF THE INVENTION

It is an object of the present invention, therefore, to provide a method and device for protecting data stored in a computing device, such as a notebook computer.

The present invention provides a device for protecting data, comprising:

an interface for connection to a computing device;

a data storage;

an encryptor located in-line between said interface and said data storage;

a control system; and

a memory that includes program data executable on said computing device to perform user authentication;

wherein said control system is configured to expose said memory to said interface to facilitate user authentication and at least until user authentication and to expose said encryptor to said interface only upon successful user authentication, and said encryptor is operable to encrypt on the fly data received from said interface and to forward said data once encrypted to said data storage and to decrypt on the fly data received from said data storage and to forward said data once decrypted to said interface.

Thus, the data stored in the data storage is encrypted, but the user need not be aware of the encryption or decryption processes.

In one embodiment, the control system is configured to reboot said computing device after successful user authentication and before exposing said encryptor to said interface.

The memory may comprise a portion of a memory storage system provided with one or more bootable programs.

The computing device could be any such device, but the invention will provide particular benefit with portable computing devices that - as discussed above - are most vulnerable to unauthorized data access.

The present invention also provides a device for protecting data, comprising:

a first interface for connection to a computing device;

a second interface for connection to a data storage;

an encryptor located in-line between said first interface and said second interface;

a control system; and

a memory that includes program data executable on said computing device to perform user authentication;

wherein said control system is configured to expose said memory to said first interface to facilitate user authentication and at least until user authentication and to expose said encryptor to said first interface only upon successful user authentication, and said encryptor is operable to encrypt on the fly data received from said first interface and to forward said data once encrypted to said second interface and to decrypt on the fly data received from said second interface and to forward said data once decrypted to said first interface.

The present invention also provides a method of protecting data, comprising:

locating an encryptor in-line between a data storage and an interface to a computing device;

exposing a memory to said interface to facilitate user authentication and at least until user authentication;

exposing said encryptor to said interface only upon successful user authentication;

encrypting on the fly data received from said first interface and forwarding said data once encrypted to said second interface; and

decrypting on the fly data received from said second interface and forwarding said data once decrypted to said first interface.

BRIEF DESCRIPTION OF THE DRAWINGS

In order that the invention may be more clearly ascertained, preferred embodiments will now be described, by way of example, with reference to the accompanying drawings, in which:

Figure 1 is a schematic view of a data protection device according to an embodiment of the present invention, with a portable computing device with which the device is to be used;

Figure 2 is a photograph of one embodiment of the data protection device of figure 1; and

Figure 3 is a schematic view of the functional components of the data protection device of figure 1;

Figure 4 is a schematic view of the functional

CLAIMS:

1. A device for protecting data, comprising:

an interface for connection to a computing device;

a data storage;

an encryptor located in-line between said interface and said data storage;

a control system; and

a memory that includes program data executable on said computing device to perform user authentication;

wherein said control system is configured to expose said memory to said interface to facilitate user authentication and at least until user authentication and to expose said encryptor to said interface only upon successful user authentication, and said encryptor is operable to encrypt on the fly data received from said interface and to forward said data once encrypted to said data storage and to decrypt on the fly data received from said data storage and to forward said data once decrypted to said interface.

2. A device as claimed in claim 1, wherein said control system is configured to reboot said computing device after successful user authentication and before exposing said encryptor to said interface.

3. A device as claimed in claim 1, wherein said memory comprises a portion of a memory storage system provided with one or more bootable programs.

4. A device for protecting data, comprising:

a first interface for connection to a computing device;

a second interface for connection to a data storage;

an encryptor located in-line between said first interface and said second interface;

a control system; and

a memory that includes program data executable on said computing device to perform user authentication;

wherein said control system is configured to expose said memory to said first interface to facilitate user authentication and at least until user authentication and to expose said encryptor to said first interface only upon successful user authentication, and said encryptor is operable to encrypt on the fly data received from said first interface and to forward said data once encrypted to said second interface and to decrypt on the fly data received from said second interface and to forward said data once decrypted to said first interface.

5. A device as claimed in claim 4, wherein said control system is configured to reboot said computing device after successful user authentication and before exposing said encryptor to said first interface.

6. A method of protecting data, comprising:

locating an encryptor in-line between a data storage and an interface to a computing device;

exposing a memory to said interface to facilitate user authentication and at least until user authentication;

exposing said encryptor to said interface only upon successful user authentication;

encrypting on the fly data received from said first interface and forwarding said data once encrypted to said second interface; and

decrypting on the fly data received from said second interface and forwarding said data once decrypted to said first interface.

7. A device as claimed in either claim 1 or 4, wherein said memory includes a bootable program configured to automatically load into said computing device when said device is connected to said computing device and said computing device is powered up.